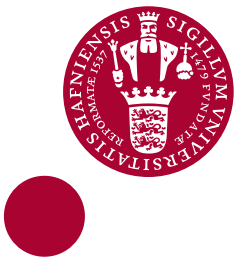
UNIVERSITY OF COPENHAGEN



Nondeterministic quantum communication complexity

The cyclic equality game and iterated matrix multiplication

Buhrman, Harry; Christandl, Matthias; Zuiddam, Jeroen

Published in:
8th Innovations in Theoretical Computer Science Conference, ITCS 2017

DOI:
10.4230/LIPIcs.ITCS.2017.24

Publication date:
2017

Document version
Publisher's PDF, also known as Version of record

Document license:
CC BY

Citation for published version (APA):
Buhrman, H., Christandl, M., & Zuiddam, J. (2017). Nondeterministic quantum communication complexity: The cyclic equality game and iterated matrix multiplication. In C. H. Papadimitriou (Ed.), *8th Innovations in Theoretical Computer Science Conference, ITCS 2017* (pp. 1-18). [24] Schloss Dagstuhl - Leibniz-Zentrum für Informatik. Leibniz International Proceedings in Informatics, LIPIcs Vol. 67
https://doi.org/10.4230/LIPIcs.ITCS.2017.24

Download date: 04. May. 2023

Nondeterministic Quantum Communication Complexity: the Cyclic Equality Game and Iterated Matrix Multiplication*

Harry Buhrman[1], Matthias Christandl[2], and Jeroen Zuiddam[3]

1 **QuSoft, CWI and University of Amsterdam, Amsterdam, The Netherlands**
buhrman@cwi.nl
2 **QMATH, Department of Mathematical Sciences, University of Copenhagen, Copenhagen, Denmark**
christandl@math.ku.dk
3 **QuSoft, CWI and University of Amsterdam, Amsterdam, The Netherlands**
j.zuiddam@cwi.nl

Abstract

We study nondeterministic multiparty quantum communication with a quantum generalization of broadcasts. We show that, with number-in-hand classical inputs, the communication complexity of a Boolean function in this communication model equals the logarithm of the *support rank* of the corresponding tensor, whereas the approximation complexity in this model equals the logarithm of the *border support rank*. This characterisation allows us to prove a log-rank conjecture posed by Villagra et al. for nondeterministic multiparty quantum communication with message passing.

The support rank characterization of the communication model connects quantum communication complexity intimately to the theory of asymptotic entanglement transformation and algebraic complexity theory. In this context, we introduce the *graphwise equality problem*. For a cycle graph, the complexity of this communication problem is closely related to the complexity of the computational problem of multiplying matrices, or more precisely, it equals the logarithm of the support rank of the iterated matrix multiplication tensor. We employ Strassen's laser method to show that asymptotically there exist nontrivial protocols for every odd-player cyclic equality problem. We exhibit an efficient protocol for the 5-player problem for small inputs, and we show how Young flattenings yield nontrivial complexity lower bounds.

1998 ACM Subject Classification E.4 Coding and Information Theory

Keywords and phrases Quantum communication complexity, broadcast channel, number-in-hand, matrix multiplication, support rank

Digital Object Identifier 10.4230/LIPIcs.ITCS.2017.24

1 Introduction

Let $f : X \times Y \times Z \to \{0, 1\}$ be a function on a product of finite sets X, Y and Z. Alice, Bob and Charlie have to compute f in the following sense. Alice receives an $x \in X$, Bob

* Part of this work was done while MC and JZ were visiting the Simons Institute for the Theory of Computing, UC Berkeley. HB was partially funded by the European Commission, through the SIQS project and by the Netherlands Organisation for Scientific Research (NWO) through gravitation grant Networks. MC acknowledges financial support from the European Research Council (ERC Grant Agreement no 337603), the Danish Council for Independent Research (Sapere Aude) and VILLUM FONDEN via the QMATH Centre of Excellence (Grant No. 10059). Part of this work was done while MC was with ETH Zurich. JZ is supported by NWO through the research programme 617.023.116 and by the European Commission through the SIQS project


© Harry Buhrman, Matthias Christandl, and Jeroen Zuiddam;
licensed under Creative Commons License CC-BY

receives a $y \in Y$ and Charlie receives a $z \in Z$, and each player receives a private random bit string. Then the players communicate in rounds. Each round, one player communicates by broadcasting a bit to the other players. After these rounds of communication, each player has to output a bit, such that if $f(x, y, z) = 1$, then with some nonzero probability all players output 1 and if $f(x, y, z) = 0$, then with probability zero all players output 1. The complexity of such a protocol is the number of broadcasts in the protocol, and we denote the minimum complexity of all such protocols by $\mathrm{N}(f)$.

Now we allow the players to be quantum, as follows. Alice receives an $x \in X$, Bob receives a $y \in Y$ and Charlie receives a $z \in Z$. Then, the players communicate by creating a GHZ state of rank r

$$|\mathrm{GHZ}_r\rangle = \tfrac{1}{\sqrt{r}}(|111\rangle + |222\rangle + \cdots + |rrr\rangle).$$

and sharing this state among each other, a quantum broadcast. Next, the players do local quantum operations. Finally, each player has to output a bit, such that if $f(x, y, z) = 1$, then with some nonzero probability all players output 1 and if $f(x, y, z) = 0$, then with probability zero all players output 1. The quantum complexity of such a quantum protocol is $\log_2 r$, and we denote the minimum complexity of all quantum protocols by $\mathrm{NQ}(f)$. We will make this definition more precise and more general in Section 2. Note that the quantum model can simulate the classical model by a postselection procedure. Also note that, nondeterministically, one quantum broadcast can be used to send a qubit from one player to another by using teleportation (see Theorem 8); the quantum model can thus simulate a message-passing model. The classical and quantum communication model naturally extend to k players.

1.1 Our results

- Our main technical result is that the quantum complexity of a function in the above model equals the logarithm of the so-called *support rank* of the tensor $\sum_{x,y,z} f(x, y, z)\,|x\rangle|y\rangle|z\rangle$ corresponding to f. We prove this in Section 2.
- Modifying the quantum model such that the players can only communicate by message passing and there is no shared $|\mathrm{GHZ}_r\rangle$ at the start – that is, the players now communicate in rounds and in each communication round one player sends a qubit to one other player – increases the complexity by at most a factor $k - 1$ (with k the number of players), and this relationship is tight. However, asymptotically in the input size, the increase is only $k/2$ and this relationship is tight. This solves a *nondeterministic multiplayer quantum log-rank conjecture* in the message-passing model of Villagra et al. [19]. This topic is covered in Section 3.
- We define the k-player *graphwise equality* problem to be the problem in which k players are identified with vertices in a graph G, and each player has to compute the equality function with his neighbours in G. Of particular interest is the cycle graph $G = C_k$ and the corresponding *cyclic equality* problem. For this cyclic equality problem, in the classical broadcast model, the naïve protocol in which every player broadcasts his inputs is the optimal protocol. The same holds in the quantum model when k is even. Interestingly, we show with Strassen's laser method that for all odd $k \geq 3$ there is a nontrivial quantum protocol. Moreover, for all odd $k \geq 3$ we give nontrivial lower bounds on the value of NQ by use of Young flattenings. These results are related to the complexity of matrix multiplication and iterated matrix multiplication. In particular, we improve a lower bound of Ikenmeyer on the border support rank of IMM_n^3 [11, 8.2.17]. A consequence of our work is that finding new protocols for the cyclic equality problem for three players yields new algorithms for matrix multiplication. Section 4 covers the classical case, the even quantum case, an explicit quantum protocol for $k = 5$, and the Young flattening lower bound. Section 5 covers the Strassen laser method.

1.2 Related work

The two-player nondeterministic quantum communication model was introduced by De Wolf [21]. He shows that the communication complexity in this model is characterized by the logarithm of the support rank of the communication matrix. The quantum broadcast channel, a communication model that is very similar to ours, has been studied by e.g. Ambainis et al. [1]. Multiparty nondeterministic quantum communication with message passing has been studied by Villagra et al. [19]. They show that the logarithm of the support rank of the communication tensor is a lower bound for the message-passing complexity and conjecture that this lower bound is polynomially related to the message-passing complexity.

The support rank of 3-tensors has been studied by Cohn and Umans in the context of the complexity of matrix multiplication [9]. They give nontrivial upper bounds on the support rank of the matrix multiplication tensor that do not come from upper bounds on the tensor rank. As an interesting fact, we note that given a matrix A and a number k, deciding whether the support rank of A is at least k is NP-hard [3].

The complexity of matrix multiplication plays a central role in algebraic complexity theory. We refer to [6] for general background information. Connections between algebraic complexity theory and entanglement transformations have been studied before, see for example [7]. The iterated matrix multiplication tensor has been studied in the context of arithmetic circuit complexity and the VP versus VNP problem, see for example [10]. To the knowledge of the authors, the tensor rank or support rank of the iterated matrix multiplication tensor has not been studied before.

Our work has motivated the further investigation of the tensor rank tensors defined by cycle graphs and more general graphs [8], which in turn when used in conjunction with this paper, lead to improved bounds on the non-deterministic quantum communication complexity of the cyclic equality game and more generally equality games played on graphs.

2 Support rank characterization of the quantum broadcast model

We refer to Nielsen and Chuang [15] for background information on the quantum computation model.

Quantum multiparty communication protocol. For any natural number m, denote by $[m]$ the set $\{1, 2, \ldots, m\}$. Let k be a positive integer and let f be a Boolean function on $[2^n]^k = [2^n] \times [2^n] \times \cdots \times [2^n]$,

$$f : [2^n]^k \to \{0, 1\}.$$

We define a *k-player quantum communication protocol* as follows. Each player i has a finite-dimensional Hilbert space H_i. The protocol thus takes place in the space $H_1 \otimes \cdots \otimes H_k$. The space is initialised in the state $|x_1 \cdots x_k\rangle |\mathrm{GHZ}_r^k\rangle$, where

$$|\mathrm{GHZ}_r^k\rangle \coloneqq \sum_{a=1}^{r} |a\rangle|a\rangle \cdots |a\rangle \in (\mathbf{C}^r)^{\otimes k}$$

is the k-party GHZ-state of rank r, shared among the k players, and $x_i \in [2^n]$ is the classical input to player i. (For clarity we will suppress any normalizations in quantum states when possible.) The players now apply local quantum operations. Let R_i be the first qubit of H_i and let $R = R_1 \otimes \cdots \otimes R_k$. We apply a projection onto $|11 \cdots 1\rangle$ in R. If the resulting tensor is 0 then the output of the protocol is 0, otherwise the output of the protocol is 1. The

complexity of the protocol is $\log_2(r)$. We say the protocol *nondeterministically computes* f if the probability that the output equals 1 is nonzero if $f(x_1, \ldots, x_k) = 1$ and the probability that the output equals 0 is one if $f(x_1, \ldots, x_k) = 0$.

▶ **Definition 1.** Let k be a positive integer and let f be a function $[2^n]^k \to \{0, 1\}$. The *k-player nondeterministic quantum communication complexity of f* is the minimal complexity of a k-player quantum communication protocol that nondeterministically computes f, and is denoted by $\mathrm{NQ}(f)$.

Approximating protocols. Let f be a function $[2^n]^k \to \{0, 1\}$. Let $(\Pi_j)_{j \in \mathbf{N}}$ be a sequence of protocols, such that when $f(x_1, \ldots, x_k) = 1$, the probability that Π_j outputs 1 on input x converges to a nonzero number as j goes to infinity, and when $f(x_1, \ldots, x_k) = 0$, the probability that Π_j outputs 0 on input x converges to 1 as j goes to infinity. Then we say that the sequence $(\Pi_j)_{j \in \mathbf{N}}$ *approximately nondeterministically computes* f. The complexity of an approximating sequence is the maximum complexity of any protocol Π_j in the sequence.

▶ **Definition 2.** The *k-player approximate nondeterministic quantum communication complexity of f* is the minimal complexity of a sequence (Π_j) that approximately nondeterministically computes f, and is denoted by $\underline{\mathrm{NQ}}(f)$.

Classical protocol. We define a *k-player classical communication protocol* as follows. Each player receives a classical input and a private random bit string. The protocol proceeds in rounds. Each round we let a single predetermined player communicate by broadcasting a bit to all the other players. After the last communication round, every player presents an output bit. If all the output bits are 1, then the output of the protocol is 1; otherwise the output of the protocol is 0. Again, we say the classical protocol *nondeterministically computes* f if the probability that the output equals 1 is nonzero if $f(x_1, \ldots, x_k) = 1$ and the probability that the output equals 0 is one if $f(x_1, \ldots, x_k) = 0$.

▶ **Definition 3.** The *k-player nondeterministic classical communication complexity of f* is the minimal complexity of a k-player classical communication protocol that nondeterministically computes f, and is denoted by $\mathrm{N}(f)$.

▶ Remark. For simplicity, we have taken the input set for each of the k players to be the same set $[2^n]$. We note that the definitions in this section and most of the results in this paper naturally generalize to the situation where the players get inputs from sets of different sizes.

Support rank and border support rank. Let t be a tensor in $(\mathbf{C}^m)^{\otimes k}$. The *tensor rank* of t is the smallest number r such that t can be written as a sum of r simple tensors, that is, $t = \sum_{i=1}^{r} u_i^1 \otimes u_i^2 \otimes \cdots \otimes u_i^k$ for some vectors $u_i^j \in \mathbf{C}^m$. We denote the tensor rank of t by $\mathrm{R}(t)$. Let $|1\rangle, \ldots, |m\rangle$ be the standard basis for $\mathbf{C}^m$ and define the support of a tensor t in $(\mathbf{C}^m)^{\otimes k}$ to be the set of product basis elements $|i_1\rangle \otimes \cdots \otimes |i_k\rangle$ that occur with nonzero coefficient in t. The *support rank* or *nondeterministic rank* of t is the smallest number r such that there exists a tensor in the space $(\mathbf{C}^m)^{\otimes k}$ with the same support as t and tensor rank r. We denote the support rank of t by $\mathrm{R_s}(t)$. Note that support rank is basis *dependent*.

The *border rank* of t is the smallest number r such that there exists a sequence of tensors $(t_j)_{j \in \mathbf{N}}$ converging to t in the Euclidean topology (or equivalently in the Zariski topology) such that $\mathrm{R}(t_j)$ is at most r for every j. We denote the border rank of t by $\underline{\mathrm{R}}(t)$. The *border support rank* of t is the smallest number r such that there exists a tensor in $(\mathbf{C}^m)^{\otimes k}$ with the same support as t and border rank r. We denote the border support rank of t by $\underline{\mathrm{R}}_{\mathrm{s}}(t)$.

▶ **Theorem 4.** *Let $f : [2^n]^k \to \{0,1\}$ be a function and let t be the tensor in $(\mathbf{C}^{2^n})^{\otimes k}$ with entries given by f, that is, $t = \sum_{i \in [2^n]^k} f(i)\,|i_1\rangle|i_2\rangle \cdots |i_k\rangle$. Then $\mathrm{NQ}(f) = \log_2 \mathrm{R_s}(t)$ and $\underline{\mathrm{NQ}}(f) = \log_2 \underline{\mathrm{R}}_{\mathrm{s}}(t)$.*

▶ **Lemma 5** (Cleanup lemma)**.** *Let $\{|\psi_i\rangle : i \in [q]\} \subseteq (\mathbf{C}^m)^{\otimes k}$ be a set of k-tensors, for some natural number q. Then there exists a k-partite rank-1 linear map $\langle \ell| \coloneqq \langle \ell_1| \otimes \cdots \otimes \langle \ell_k|$ with $\langle \ell_j| \in (\mathbf{C}^m)^*$ such that $\langle \ell|\psi_i\rangle \neq 0$ for every $i \in [q]$.*

Proof. We will give a proof by recursively constructing $\langle \ell|$. Let Id be the identity map on $\mathbf{C}^m$. If $j \leq k$, $\langle a| \in ((\mathbf{C}^m)^*)^{\otimes j}$ and $|b\rangle \in (\mathbf{C}^m)^{\otimes k}$, then we denote by $\langle a|b\rangle$ the contraction of $\langle a|$ and $|b\rangle$, that is, $\langle a|b\rangle = (\langle a| \otimes \mathrm{Id}^{\otimes k-j})\,|b\rangle$.

The base case is $\langle \ell| = 1$. For the recursion, suppose we are given an element $\langle \ell'| \in ((\mathbf{C}^m)^*)^{\otimes j}$ such that $|\phi_i\rangle \coloneqq \langle \ell'|\psi_i\rangle$ is nonzero for every $i \in [q]$. We will construct an element $\langle \ell| \in ((\mathbf{C}^m)^*)^{\otimes j+1}$ such that $\langle \ell|\psi_i\rangle$ is nonzero for every $i \in [q]$. Since $|\phi_i\rangle$ is nonzero for every $i \in [q]$, there is an element $\langle u_i| \in (\mathbf{C}^m)^*$ such that $\langle u_i|\phi_i\rangle$ is nonzero. Consider the the maps $(\langle u_1| + x\,\langle u_2|)\,|\phi_i\rangle$ for $i \in \{1,2\}$, in the variable x. Each map only has a single root. Therefore, there exists a value α_2 for x such that both maps evaluate to a nonzero number. Next, consider the maps $(\langle u_1| + \alpha_2\,\langle u_2| + x\,\langle u_3|)\,|\phi_i\rangle$ for $i \in \{1,2,3\}$, in variable x. Again, each of the three maps has only a single root. Therefore, there exists a value α_3 for x such that all three maps evaluate to a nonzero number. Repeat this construction to obtain an element $\langle u| \in (\mathbf{C}^m)^*$ such that $\langle u|\phi_i\rangle$ is nonzero for every $i \in [q]$. Let $\langle \ell|$ be $\langle \ell'| \otimes \langle u|$. ◀

Proof of Theorem 4. We first show $\mathrm{NQ}(f) \leq \log_2 \mathrm{R_s}(t)$. Let r be the support rank of t. Then there exists a unit vector $\psi \in (\mathbf{C}^{2^n})^{\otimes k}$ with rank r and support equal to the support of f. This means that there are vectors $|u_i^j\rangle \in \mathbf{C}^{2^n}$ such that $\psi = \sum_{i=1}^r |u_i^1\rangle \cdots |u_i^k\rangle$. For every player j define a matrix

$$A_j \coloneqq \alpha_j \sum_{i=1}^{r} |u_i^j\rangle\langle i|$$

where α_j is a nonzero complex number such that $A_j^\dagger A_j$ has eigenvalue at most 1. The matrix $I - A_j^\dagger A_j$ is thus positive semidefinite and hence there exists a matrix A_j' such that ${A_j'}^\dagger A_j' = I - A_j^\dagger A_j$. Define for every player j a quantum operation

$$\mathcal{E}_j : \rho \mapsto A_j \rho A_j^\dagger \otimes |1\rangle\langle 1| + A_j' \rho {A_j'}^\dagger \otimes |0\rangle\langle 0|\,.$$

Note that this operation introduces a new control qubit register which player j can measure to see whether he applied A_j or A_j'.

The protocol for the k players is as follows. Let $x_1, \ldots, x_k$ be the inputs given to the players. The players share a k-party GHZ-state of rank r. Player j applies $\mathcal{E}_j$ to his part of the GHZ-state. If his control qubit is $|0\rangle$ then he sets his output qubit R_i to $|0\rangle$. Otherwise, he measures the rest of the system. If the outcome equals $|x_j\rangle$, then he sets R_j to $|1\rangle$, otherwise he sets R_j to $|0\rangle$.

The above protocol uses a GHZ-state of rank r, so it has complexity $\log_2(r)$. We claim that the protocol nondeterministically computes f. If the players in the first measurement each get outcome $|1\rangle$, then the state of the total system is $|\psi\rangle$. Because $|\psi\rangle$ has norm 1, this happens with nonzero probability $|\alpha_1|^2 \cdots |\alpha_k|^2$. If $f(x_1, \ldots, x_k) = 0$, then $|x_1 \cdots x_k\rangle$ does not occur in the support of ψ, so the probability that the players measure $|x_1\rangle, \ldots, |x_k\rangle$ respectively is zero. Hence in this case the register R is not in state $|11\cdots1\rangle$. On the other hand, if $f(x_1, \ldots, x_k) \neq 0$, then $|x_1 \cdots x_k\rangle$ does occur in the support of ψ, so the probability that the players measure $|x_1\rangle, \ldots, |x_k\rangle$ respectively is nonzero. Hence with nonzero probability the register R is in state $|11\cdots1\rangle$.

We now show $\mathrm{NQ}(f) \geq \log_2 \mathrm{R_s}(t)$. Suppose we have a protocol that nondeterministically computes f with complexity r. This means that the players perform *local* quantum operations that together form a linear map L which transforms, for any $x_1, \ldots, x_k \in [2^n]$, the state

$$|x_1 \cdots x_k\rangle \, |\mathrm{GHZ}_r\rangle$$

to a state of the form

$$|x_1 \cdots x_k\rangle \sum_{a \in \{0,1\}^k} |\psi_x^a\rangle \; |a_1\rangle |a_2\rangle \cdots |a_k\rangle \,,$$

where $|\psi_x^a\rangle$ is some vector representing the state of the work space of the players. By definition of nondeterministic computation, for $a = (1, \ldots, 1)$, if $f(x_1, \ldots, x_k) = 1$, then $|\psi_x^a\rangle$ is nonzero, and if $f(x_1, \ldots, x_k) = 0$, then $|\psi_x^a\rangle$ is zero. Since the map L is linear, it maps the tensor

$$s_1 \coloneqq \sum_{x_1, \ldots, x_k} |x_1 \cdots x_k\rangle \, |\mathrm{GHZ}_r\rangle$$

to the tensor

$$s_2 \coloneqq \sum_{x_1, \ldots, x_k} |x_1 \cdots x_k\rangle \sum_{a \in \{0,1\}^k} |\psi_x^a\rangle \, |a_1 \cdots a_k\rangle \,.$$

The tensor rank of $\sum_x |x_1 \cdots x_k\rangle$ is 1 and hence the tensor rank of s_1 is r. Because L is a local map, the tensor rank of s_2 is at most r. By applying the cleanup lemma (Lemma 5) and projecting on states with $|a_1 \cdots a_k\rangle = |1 \cdots 1\rangle$, we obtain a tensor

$$s_3 \coloneqq \sum_{x_1, \ldots, x_k} |x_1 \cdots x_k\rangle \, c_x$$

where $c_x \in \mathbf{C}$ is zero if $f(x) = 0$ and nonzero if $f(x) = 1$. The rank of the tensor s_3 is at most r. The support of s_3 equals the support of f, so the support rank of f is at most r.

The statement about the approximate complexity of f follows from the definition of border support rank. ◀

▶ **Definition 6** (SLOCC)**.** Let $\phi \in U_1 \otimes \cdots \otimes U_k$ and let $\psi \in V_1 \otimes \cdots \otimes V_k$. We say that ϕ can be converted to ψ by stochastic local operations and classical communication (SLOCC), and write $\phi \xrightarrow{\mathrm{SLOCC}} \psi$, if there exist matrices $A_1, \ldots, A_k$ such that $\psi = (A_1 \otimes \cdots \otimes A_k)\phi$.

▶ Remark. We note that having an NQ-protocol for f of complexity n is the same as having an SLOCC protocol for transforming $\mathrm{GHZ}_{2^n}^k$ to a tensor with the same support as f. We will use the SLOCC paradigm in some parts of the text.

▶ Remark. The NQ-model that we are using is very similar to the following *broadcast channel* model that was studied in [1]. Each player i has a local Hilbert space H_i with a register initialised in the input state $|x_i\rangle$. The players have access to a quantum broadcast channel, which, given a qubit state $\alpha |0\rangle + \beta |1\rangle$, will create the state $\alpha |0\rangle^{\otimes k} + \beta |1\rangle^{\otimes k}$ and distribute this state among the k players. The players proceed in communication rounds; each round a designated player uses the broadcast channel. Let R_i be the first qubit of H_i and let $R = R_1 \otimes \cdots \otimes R_k$. After the communication is finished, we apply a projection onto $|11 \cdots 1\rangle$ in R. If the resulting tensor is 0 then the output of the protocol is 0, otherwise the output of the protocol is 1. The complexity of the protocol is the number of communication rounds. We say the protocol nondeterministically computes f if the probability that the output equals 1 is nonzero if $f(x_1, \ldots, x_k) = 1$ and the probability that the output equals 0 is one if $f(x_1, \ldots, x_k) = 0$.

In particular, let $\mathrm{NQ}'(f)$ denote the complexity of the function f in the broadcast channel model. Then $\mathrm{NQ}'(f) \leq \mathrm{NQ}(f) + 1$. Indeed, consider a protocol in the NQ-model that computes f using $|\mathrm{GHZ}_r^k\rangle$ as a starting state. To simulate this protocol in the NQ'-model, one of the players uses the broadcast channel $\lceil \log_2 r \rceil$ times to create $|\mathrm{GHZ}_r^k\rangle$. Then the players proceed with the local quantum operations to compute f. This finishes the proof. We don't know whether the inequality $\mathrm{NQ}(f) \leq \mathrm{NQ}'(f)$ holds.

3 Nondeterministic log-rank conjecture for message-passing protocols

▶ **Definition 7.** Let $\mathrm{NQ}_0(f)$ be the minimal complexity of a protocol that nondeterministically computes f, without preshared entanglement (that is, the space is initialised in the state $|x_1 \cdots x_k\rangle$ instead of $|x_1 \cdots x_k\rangle |\mathrm{GHZ}_r^k\rangle$) but with the added ability for every player to send a qubit to another player. This communication happens in communication rounds; the protocol specifies per round who communicates to whom, independently of the input. The complexity of such a protocol is the total number rounds.

Villagra et al. [19] show that $\mathrm{NQ}_0(f)$ is at least the logarithm of the support rank of f. They furthermore conjecture that $\mathrm{NQ}_0(f)$ is upper bounded by a polynomial in the logarithm of the support rank. The following theorem proves this conjecture.

▶ **Theorem 8** ("Nondeterministic log-rank conjecture"). *Let $f : [2^n]^k \to \{0,1\}$. Then we have $\mathrm{NQ}(f) \leq \mathrm{NQ}_0(f) \leq (k-1)\,\mathrm{NQ}(f)$.*

Proof. For the first inequality, suppose we have an NQ_0-protocol for f. We replace the communication of a qubit by the nondeterministic teleportation of that qubit. Beforehand, all players agree on the basis in which the teleportation should happen. If any teleportation during the protocol does not happen in this basis, then the player that notices this sets his output register R_i to $|0\rangle$.

For the second inequality, suppose we have an NQ-protocol for f which uses a GHZ-state of rank r. Then we can construct a NQ_0-protocol for f as follows. The players start with no shared entanglement. Player 1 constructs a GHZ-state of rank r locally. In the first $k-1$ communication rounds, player 1 distributes the GHZ-state over the other $k-1$ players. After that, the players perform the NQ-protocol. The resulting NQ_0-protocol has complexity at most $(k-1)\,\mathrm{NQ}(f)$. ◀

To say something about the 'tightness' of Theorem 8 we consider the natural easy function in the NQ-model, namely $f(x_1, \ldots, x_k) = [x_1 = x_2 = \cdots = x_k]$ with $x_i \in [2^n]$.

▶ **Proposition 9** (Single bit inputs). *Let $f : [2]^k \to \{0,1\}$ be the function defined by $f(x_1, \ldots, x_k) = [x_1 = x_2 = \cdots = x_k]$ for $x_i \in [2]$. Then we have $\mathrm{NQ}(f) = 1$ and $\mathrm{NQ}_0(f) = (k-1)\,\mathrm{NQ}(f)$.*

Proof. Note that the tensor of this function is GHZ_2^k, so $\mathrm{NQ}(f) = 1$. Now consider a protocol that nondeterministically computes f without preshared entanglement and r rounds of communication. We may assume, without loss of generality, that the protocol consists of a first phase in which the players communicate and a second phase in which the players only do local quantum operations. After the first phase the players are sharing some state E consisting of EPR-pairs shared among certain pairs of the players. We thus obtain a local linear map which maps $\sum_x |x\rangle\, E$ to a tensor with the same support as GHZ_2^k. However, if $r < k-1$, then, viewing E as a graph, E is disconnected. Therefore there is a grouping of the players into two groups such that there are no EPR-pairs between the groups. Such a state cannot be converted to a GHZ_2^k state by SLOCC. ◀

Asymptotically, we can improve the relationship stated in Theorem 8, as follows.

▶ **Theorem 10** (Asymptotic upper bound). *For any $\varepsilon > 0$, there is an n_0 such that for all $f : [m]^k \to \{0,1\}$, if $\mathrm{NQ}(f) > n_0$, then*

$$\mathrm{NQ}_0(f) \leq \frac{(k+\varepsilon)}{2}\,\mathrm{NQ}(f).$$

To prove Theorem 10 we use the theory of asymptotic SLOCC conversion rates.

▶ **Definition 11.** Given tensors $\psi \in V_1 \otimes \cdots \otimes V_k$ and $\phi \in W_1 \otimes \cdots \otimes W_k$, we say that ψ can be transformed into ϕ via SLOCC operations, if there exist linear transformations $A_i : V_i \to W_i$ such that $\phi = (A_1 \otimes \cdots \otimes A_k)\psi$; and we write $\psi \xrightarrow{\text{SLOCC}} \phi$. Define

$$\omega_n(\psi,\phi) = \frac{1}{n}\inf\{m \in \mathbf{N}_{\geq 1} \mid \psi^{\otimes m} \xrightarrow{\text{SLOCC}} \phi^{\otimes n}\}$$

and

$$\omega(\psi,\phi) = \lim_{n\to\infty} \omega_n(\psi,\phi).$$

▶ **Lemma 12.** *The limit $\omega(\psi,\phi)$ exists and for all n the inequality $\omega_n(\psi,\phi) \geq \omega(\psi,\phi)$ holds; in other words, $\omega_n = \omega + o(1)$.*

▶ **Theorem 13** (Vrana-Christandl [20]). *Let $\mathrm{GHZ}_2^{K_k}$ be the k-party tensor consisting of EPR-pairs between any parties. Then*

$$\omega(\mathrm{GHZ}_2^{K_k}, \mathrm{GHZ}_2^k) = \frac{1}{k-1}.$$

In other words, for any $\varepsilon > 0$, there is an n_0 such that for all $n > n_0$,

$$(\mathrm{GHZ}_2^{K_k})^{\otimes n(\frac{1}{k-1}+\varepsilon)} \xrightarrow{\text{SLOCC}} (\mathrm{GHZ}_2^k)^{\otimes n}.$$

Proof of Theorem 10. Creating $\mathrm{GHZ}_2^{K_k}$ in the NQ_0-model costs $\binom{k}{2}$ messages. Asymptotically, we can transform $1/(k-1)$ copies of $\mathrm{GHZ}_2^{K_k}$ to one copy of GHZ_2^k by SLOCC. More precisely, by Theorem 13, for any $\varepsilon > 0$, there is an n_0 such that for all $n > n_0$,

$$(\mathrm{GHZ}_2^{K_k})^{\otimes \frac{n}{k-1}+\varepsilon n} \xrightarrow{\text{SLOCC}} (\mathrm{GHZ}_2^k)^{\otimes n}.$$

We conclude that, for any $\varepsilon > 0$, there is an n_0 such that for all $n > n_0$, $\binom{k}{2}(\frac{n}{k-1} + \varepsilon n) = ((k+\varepsilon')n)/2$ messages are sufficient to generate $(\mathrm{GHZ}_2^k)^{\otimes n}$ by SLOCC.

To prove the theorem, suppose we have an NQ-protocol for f which uses a GHZ state of rank 2^n and no communication. Consider the following NQ_0-protocol for f. Create a GHZ-state of rank 2^n by sending $\frac{(k+\varepsilon')n}{2}$ messages and then continue with the NQ-protocol. ◀

The following proposition says that the asymptotic relationship of Theorem 10 is tight.

▶ **Proposition 14** (n-bit inputs). *Let $f : [2^n]^k \to \{0,1\}$ be the function defined by $f(x_1,\ldots,x_k) = [x_1 = x_2 = \cdots = x_k]$ for $x_i \in [2^n]$. Then we have $\mathrm{NQ}(f) = n$ and $\mathrm{NQ}_0(f) \geq \frac{k}{2}\,\mathrm{NQ}(f)$.*

Proof. As in the previous proof, note that the tensor corresponding to f is $\mathrm{GHZ}_{2^n}^k$. Suppose there is an NQ_0 protocol using r messages. View the communication pattern of this protocol as an undirected multigraph G (i.e. parallel edges are allowed) on k vertices. Note that G has r edges. Let $E = \mathrm{GHZ}_2^G$ be the tensor that has an EPR pair at every edge in G. The protocol

yields an SLOCC transformation of E to $\mathrm{GHZ}_{2^n}^k$. Let ℓ be the minimal number of edges across any cut of G. Then ℓ is at most the minimal degree d of G. The sum of all degrees in G equals $2r$, so $k\ell \leq kd \leq 2r$, which implies the inequality $r \geq k\ell/2$. The number ℓ is equal to $\min_{S\subseteq[k]} \log_2 \mathrm{rk}_S(E)$, where $\mathrm{rk}_S(E)$ denotes the rank of E after flattening according to the set S. This value cannot increase under any SLOCC transformation. Now note that $\log_2 \mathrm{rk}_{\{i\}}(\mathrm{GHZ}_{2^n}^k) = n$ for any $i \in [k]$, so $\ell \geq n$. We conclude that $r \geq kn/2$. ◀

▶ Remark. Another way to prove Proposition 14 is to first symmetrize the protocol to obtain an SLOCC transformation of a state E with $\log_2 \mathrm{rk}_{\{i\}}(E) = (k-1)!2r$ to the state $\mathrm{GHZ}_{2^{k!n}}^k$. We have $\log_2 \mathrm{rk}_{\{i\}}(\mathrm{GHZ}_{2^{k!n}}^k) = k!\,n$. Since $\log_2 \mathrm{rk}_{\{i\}}$ is an SLOCC-monotone, we obtain the inequality $(k-1)!\,2r \geq k!\,n$ and hence $r \geq kn/2$.

4 Cyclic equality problem

The two-player equality problem EQ_n is the problem of Alice and Bob having to decide whether their n-bit inputs are equal. Since the identity matrix has full support rank, we have $\mathrm{NQ}(\mathrm{EQ}_n) = n$. We generalize EQ_n to multiple players as follows. Let G be an undirected graph. Let EQ_n^G be the problem of $|G|$ players having to solve the n-bit equality problem between players connected by edges. (Note that this definition naturally generalizes to hypergraphs.) If G is a bipartite graph, one easily sees that by grouping the players we can transform the problem into an equality problem on en bits EQ_{en}, where e is the number of edges in the graph. Therefore $\mathrm{NQ}(\mathrm{EQ}_n^G) = en$, that is, the trivial protocol is optimal for bipartite graphs. On the other hand, if G contains an odd cycle, then this argument fails. In the rest of this paper we will focus on the extreme case of G being an odd cycle and investigate the complexity of the corresponding equality problem.

▶ **Definition 15.** The k-player *cyclic equality problem* on n bits $\mathrm{EQ}_n^{C_k}$ is the function

$$\mathrm{EQ}_n^{C_k} : ([2^n]\times[2^n])^k \to \{0,1\} : (a_1b_1,\ldots,a_kb_k) \mapsto \begin{cases} 1 & \text{if } b_1 = a_2,\ b_2 = a_3,\ \ldots,\ b_k = a_1 \\ 0 & \text{otherwise,} \end{cases}$$

that is, the players are arranged in a circle; player i receives two n-bit inputs a_i, b_i and has to decide whether $a_i = b_{i-1}$ and $b_i = a_{i+1}$, where the indices are taken modulo k.

It turns out that the tensor corresponding to this function is a generalisation of the *matrix multiplication tensor*, one of the central objects of study in algebraic complexity theory. This tensor arises as follows in algebraic complexity theory. Consider the bilinear map

$$\mathbf{C}^{m\times m} \times \mathbf{C}^{m\times m} \to \mathbf{C}^{m\times m} : (A,B) \mapsto AB$$

which multiplies two complex $m \times m$ matrices. Any bilinear map $U \times V \to W$ corresponds canonically to a tensor in $U \otimes V \otimes W$. The number of multiplications in the field $\mathbf{C}$ necessary to perform the bilinear map is equal to the tensor rank of the corresponding tensor, up to a factor 2. The tensor corresponding to the matrix multiplication map is

$$\langle m,m,m\rangle \coloneqq \sum_{x\in[m]^3} |x_1x_2\rangle|x_2x_3\rangle|x_3x_1\rangle\,.$$

A natural generalisation of the tensor $\langle m,m,m\rangle$ to a k-party tensor is the so-called *iterated matrix multiplication* tensor

$$\mathrm{IMM}_m^k \coloneqq \sum_{x\in[m]^k} |x_1x_2\rangle|x_2x_3\rangle\cdots|x_kx_1\rangle\,.$$

Clearly, $\mathrm{IMM}_m^3 = \langle m, m, m\rangle$. The tensor IMM_m^k corresponds to the multilinear map

$$(\mathbf{C}^{m\times m})^{\times k} \to \mathbf{C} : (A_1, A_2, \ldots, A_k) \mapsto \mathrm{tr}(A_1 A_2 \cdots A_k)$$

which computes the trace of the product of k matrices. We note that, when viewed as a polynomial in the matrix entries, IMM_m^k plays a special role in the field of arithmetic circuits and geometric complexity theory. Namely, IMM_3^k is complete for the class $\mathrm{VP_e}$ of families of polynomials computable by small formulas [2], and IMM_k^k is complete for the class VQP, for which the determinant is also complete [4]. The following connection between iterated matrix multiplication and cyclic equality is readily observed.

▶ **Proposition 16.** *The tensor corresponding to the cyclic equality function* $\mathrm{EQ}_n^{C_k}$ *on* n *bits is the iterated matrix multiplication tensor* $\mathrm{IMM}_{2^n}^k$ *with* $2^n \times 2^n$ *matrices. Therefore, we have the equalities* $\mathrm{NQ}(\mathrm{EQ}_n^{C_k}) = \log_2 \mathrm{R_s}(\mathrm{IMM}_{2^n}^k)$ *and* $\underline{\mathrm{NQ}}(\mathrm{EQ}_n^{C_k}) = \log_2 \underline{\mathrm{R}}_{\mathrm{s}}(\mathrm{IMM}_{2^n}^k)$

The remainder of this paper is organized as follows. In the following four paragraphs we do the following: (1) we show that in the classical model, the naïve protocol in which every player broadcasts his input is optimal; (2) we show that when k is even the naïve protocol is optimal quantumly; (3) we exhibit nontrivial protocols when $n = 1$ and $k = 3$ or $k = 5$; (4) we show nontrivial lower bounds on the quantum complexity by use of Young flattenings. Finally, in the last section, we show that the Strassen laser method yields nontrivial protocols for all odd $k \geq 3$, asymptotically.

Classical lower bound with the fooling set method. We will show that in the classical situation the trivial protocol is always optimal. To prove a lower bound on the classical complexity of the cyclic equality problem we use the fooling set method. This is a method from the 2-player setting that extends naturally to the k-player setting.

▶ **Theorem 17.** *The classical nondeterministic communication complexity* $\mathrm{N}(\mathrm{EQ}_n^{C_k})$ *of the cyclic equality problem equals* kn*.*

Proof. Let $S \subseteq [2^{2n}]^k$ be the set of 1-inputs of the function $\mathrm{EQ}_n^{C_k}$. This set has size 2^{kn}. Let Π be a classical protocol for $\mathrm{EQ}_n^{C_k}$ and denote by $\Pi_r(x_1, \ldots, x_k)$ the sequence of messages sent by the players in the protocol Π on input $x \in [2^{2n}]^k$ and private randomness $r \in [m]^k$. Suppose there are distinct 1-inputs $x, y \in S$ and private randomnesses $r, s \in [m]^k$ such that $\Pi_r(x_1, \ldots, x_k) = \Pi_s(y_1, \ldots, y_k)$. There is an i such that $x_i \neq y_i$, say $i = 1$. We have $\Pi_r(x_1, \ldots, x_k) = \Pi_{(r_1, s_2, \ldots, s_k)}(x_1, y_2, \ldots, y_k)$, so the protocol outputs 1 on input $x_1, y_2, \ldots, y_k$ with randomness $(r_1, s_2, \ldots, s_k)$. However, $x_1, y_2, \ldots, y_k$ is a 0-input, a contradiction. Therefore, $\Pi_r(x_1, \ldots, x_k) \neq \Pi_s(y_1, \ldots, y_k)$. We conclude that $\mathrm{N}(\mathrm{EQ}_n^{C_k}) \geq \log_2(|S|)$. ◀

An even number of quantum players. When k is even, the cycle graph C_k is bipartite, and, as mentioned above, the best protocol for an equality problem on a bipartite graph is the trivial protocol. We record this statement in terms of border support rank in the following proposition.

▶ **Proposition 18.** *For even* k*,* $m^k \leq \underline{\mathrm{R}}_{\mathrm{s}}(\mathrm{IMM}_m^k)$*. As a consequence, we have the equalities* $\underline{\mathrm{NQ}}(\mathrm{EQ}_n^{C_k}) = \mathrm{NQ}(\mathrm{EQ}_n^{C_k}) = kn$*.*

Proof. Let t be a tensor with the same support as $\mathrm{IMM}_m^k \in (\mathbf{C}^{m^2})^{\otimes k}$. Label the players with the numbers $1, 2, \ldots, k$. Group the *even* players together and group the *odd* players

together and flatten the tensor t accordingly into a matrix A in $(\mathbf{C}^{m^2})^{\otimes k/2} \otimes (\mathbf{C}^{m^2})^{\otimes k/2}$. The matrix A has the same support as the identity matrix in $(\mathbf{C}^{m^2})^{\otimes k/2} \otimes (\mathbf{C}^{m^2})^{\otimes k/2}$ and thus has rank m^k. ◀

Note that for odd k the above proof yields the lower bound $m^{k-1} \leq \underline{\mathrm{R}}_{\mathrm{s}}(\mathrm{IMM}_m^k)$. We will show in Theorem 20 that this lower bound is not tight.

Nontrivial 3-player and 5-player quantum protocols. In the 3-player situation, Strassen's celebrated decomposition of the tensor $\mathrm{IMM}_2^3 = \langle 2,2,2\rangle$ into a sum of 7 simple tensors [17] gives a nontrivial protocol for $\mathrm{EQ}_1^{C_3}$, and thus $\mathrm{NQ}(\mathrm{EQ}_1^{C_3}) \leq \log_2(7)$. We show that for 5 players there also exists a nontrivial protocol for $\mathrm{EQ}_1^{C_5}$, as follows. Recall that we have defined $\mathrm{IMM}_2^5 = \sum_{i\in[2]^5} |i_1i_2\rangle|i_2i_3\rangle|i_3i_4\rangle|i_4i_5\rangle|i_5i_1\rangle$. Observe that an upper bound $\mathrm{R}(\mathrm{IMM}_2^5) \leq r$ implies $\mathrm{R}(\mathrm{IMM}_n^5) \leq \mathcal{O}(n^{\log_2(r)})$ by taking tensor powers of IMM_2^5.

▶ **Theorem 19.** $\mathrm{R}(\mathrm{IMM}_2^5) \leq 31$, *and thus* $\mathrm{NQ}(\mathrm{EQ}_1^{C_5}) \leq \log_2(31)$.

Proof. Let $|-\rangle := |1\rangle - |2\rangle$, $|+\rangle := |1\rangle + |2\rangle$ and $|\Phi^+\rangle = |11\rangle + |22\rangle$. Let $\mathrm{Cyc}_5 := \sum_{\sigma\in C_5} \sigma$ be the cyclic symmetrizer acting on $(\mathbf{C}^4)^{\otimes 5}$ by permuting the 5 parties, and moreover let $\mathrm{Sym}_2 := \sum_{\sigma\in S_2} \sigma$ be a 'local symmetrizer' acting diagonally on $(\mathbf{C}^2)^{\otimes 10}$ by permuting the basis states $|1\rangle$ and $|2\rangle$ of each $\mathbf{C}^2$. Let

$$\begin{aligned} t := &- |-1\rangle\,|11\rangle\,|11\rangle\;|1+\rangle\,|22\rangle \\ &- |-1\rangle\,|12\rangle\,|21\rangle\;|1+\rangle\,|22\rangle \\ &- |\Phi^+\rangle\,|22\rangle\,|-1\rangle|1+\rangle\,|22\rangle. \end{aligned}$$

By direct computation, we see that $\mathrm{IMM}_2^5 = \mathrm{Cyc}_5\big(\mathrm{Sym}_2(t)\big) + |\Phi^+\rangle^{\otimes 5}$. We observe that the right hand side yields a sum of 31 simple tensors. ◀

We have a proof generalizing Theorem 19 to $\mathrm{R}(\mathrm{IMM}_2^k) \leq 2^k - 1$ for all odd k, which will appear in a forthcoming paper [8].

Quantum lower bound with Young flattenings. Let $t \in V_1 \otimes V_2 \otimes V_3$ be some 3-tensor. By grouping V_1 and V_2, the tensor t can be viewed as a matrix $A \in (V_1 \otimes V_2) \otimes V_3$; this is called a *flattening*. The rank of the flattening A is a lower bound for the border rank of t and thus we obtain lower bounds on the border rank of tensors by computing the rank of their flattenings. However, this type of lower bound can never be bigger than the dimension of any local space V_i, and there do exist tensors with border rank larger than the local dimensions, for example the matrix multiplication tensor $\langle 2,2,2\rangle$.

One approach to overcome this 'local dimension limitation' is as follows. We let $\phi : V_2 \to W_1 \otimes W_2$ be a linear map such that $\mathrm{R}(\phi(v)) \leq e$ for all $v \in V_2$. By applying ϕ to the central tensor leg of t, we transform t into a 4-tensor $s \in V_1 \otimes W_1 \otimes W_2 \otimes V_3$. Next, we flatten s to a matrix $A \in (V_1 \otimes W_1) \otimes (W_2 \otimes V_3)$. The rank of A divided by e is a lower bound for the border rank of t. We will be using a specific linear map ϕ which originates from the representation theory of the general linear group. When one takes such representation theoretic maps ϕ to construct a flattening as above one speaks of a *Young flattening* [13]. An early appearance of this type of flattening can be recognized in the work of Strassen [18]. The following lower bound is obtained with a Young flattening.

▶ **Theorem 20.** *For odd* $k \geq 3$, $(2n^2 - n)n^{k-3} \leq \underline{\mathrm{R}}_{\mathrm{s}}(\mathrm{IMM}_n^k)$. *As a consequence, we have the lower bound* $(k-1)n + \log_2(2 - \frac{1}{n}) \leq \underline{\mathrm{NQ}}(\mathrm{EQ}_n^{C_k})$.

Proof. Let $k = 3$. The proof for odd $k > 3$ goes similarly after having grouped the k parties appropriately to 3 parties. For a vector space V, let $\wedge^a V$ be the ath exterior power of V. Define the linear map

$$\begin{aligned}\phi : \mathbf{C}^{2n-1} &\to \wedge^p \mathbf{C}^{2n-1} \otimes \wedge^{p+1} \mathbf{C}^{2n-1} \\ |j\rangle &\mapsto \sum_{j_1<\cdots<j_p} |j_1\rangle\wedge\cdots\wedge|j_p\rangle \otimes |j_1\rangle\wedge\cdots\wedge|j_p\rangle\wedge|j\rangle\,,\end{aligned}$$

and note that the rank of the matrix $\phi(v)$ equals $\binom{2n-2}{p}$ for any $v \in \mathbf{C}^{2n-1}$. We consider the tensor

$$t_1 \coloneqq \sum_i \alpha_{i_1,i_2,i_3} |i_1 i_2\rangle |i_2 i_3\rangle |i_3 i_1\rangle \in \mathbf{C}^{n^2} \otimes \mathbf{C}^{n^2} \otimes \mathbf{C}^{n^2},$$

where i runs over $[n]^3$ and the α_{i_1,i_2,i_3} are nonzero complex numbers. The border rank of t_1 is at least the border rank of

$$t_2 \coloneqq \sum_i \alpha_{i_1,i_2,i_3} |i_1 i_2\rangle |i_2 + i_3 - 1\rangle |i_3 i_1\rangle \in \mathbf{C}^{n^2} \otimes \mathbf{C}^{2n-1} \otimes \mathbf{C}^{n^2}.$$

Apply ϕ to the central tensor leg of t_2 and then flatten to obtain

$$A \coloneqq \sum_i \sum_{j_1<\cdots<j_p} \alpha_{i_1,i_2,i_3} |i_1 i_2\rangle |j_1\rangle\wedge\cdots\wedge|j_p\rangle \otimes |j_1\rangle\wedge\cdots\wedge|j_p\rangle\wedge|i_2 + i_3 - 1\rangle |i_3 i_1\rangle\,.$$

View A as a direct sum of n matrices $A_{i_1} \in (\mathbf{C}^n \otimes \wedge^p \mathbf{C}^{2n-1}) \otimes (\wedge^{p+1}\mathbf{C}^{2n-1} \otimes \mathbf{C}^n)$; the matrix A_{i_1} corresponds to the linear map

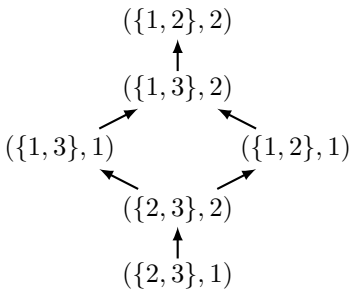
$$f_{i_1} : |i_2\rangle |j_1\rangle\wedge\cdots\wedge|j_p\rangle \mapsto \sum_{i_3} \alpha_{i_1,i_2,i_3} |j_1\rangle\wedge\cdots\wedge|j_p\rangle\wedge|i_2 + i_3 - 1\rangle |i_3\rangle\,.$$

Let $p = n - 1$. We claim that every matrix A_{i_1} is upper triangular with elements α_{i_1,i_2,i_3} on the diagonal, up to permutations of the rows and columns. Assuming the claim is true, we get that $\mathrm{R}(A) = \sum_{i_1} \mathrm{R}(A_{i_1}) = n \dim(\mathbf{C}^n \otimes \wedge^{n-1}\mathbf{C}^{2n-1}) = n^2\binom{2n-1}{n-1}$. This implies the lower bound $\underline{\mathrm{R}}_{\mathrm{s}}(\mathrm{IMM}_n^3) \geq n^2\binom{2n-1}{n-1}/\binom{2n-2}{n-1} = 2n^2 - n$.

To prove this claim we define a partial order on the basis elements $|j_1\rangle \wedge \cdots \wedge |j_n\rangle \otimes |\ell\rangle$ of the target space of A_{i_1}. We will use the same partial order as Landsberg and Michałek [12]. Denote the basis elements of the target space by (P, ℓ) with P an n-subset of $[2n-1]$ and $\ell \in [n]$. Let (P_1, ℓ_1) and (P_2, ℓ_2) be two such basis elements and define $\ell \coloneqq \min(\ell_1, \ell_2)$. We say $(P_1, \ell_1) < (P_2, \ell_2)$

1. if the ordered sequence of the ℓ smallest elements in P_2 is lexicographically smaller than the ordered sequence of the ℓ smallest elements in P_1;
2. or if the sequences of ℓ smallest elements are equal and $\ell_1 < \ell_2$.

One checks that this defines a partial order and that the unique minimal element in this order is $(\{n, \ldots, 2n-1\}, 1)$. For example, with $n = 2$ the partial order has the following Hasse diagram.



We prove the claim by induction on $<$, with the minimal element as a base case. For now let all the α_{i_1,i_2,i_3} be 1. First, under A_{i_1} we have

$$|n\rangle \otimes |n+1\rangle \wedge \cdots \wedge |2n-1\rangle \mapsto |n\rangle \wedge \cdots \wedge |2n-1\rangle \otimes |1\rangle\,,$$

so the minimal element $(\{n,\dots,2n-1\},1)$ is in the image of A_{i_1}. Let (P,ℓ) be in the target space of A_{i_1} and assume that every (P',ℓ') with $(P',\ell') < (P,\ell)$ is in the image. Write $P=(p_1,\dots,p_n)$ with $p_1 \le \cdots \le p_n$. Under A_{i_1} we have,

$$|p_1\rangle \wedge \cdots \widehat{p_\ell} \cdots \wedge |p_n\rangle \otimes |1+p_\ell-\ell\rangle \mapsto \sum_m |p_1\rangle \wedge \cdots \widehat{p_\ell} \cdots \wedge |p_n\rangle \wedge |p_\ell-\ell+m\rangle \otimes |m\rangle\,.$$

Taking $m=\ell$, one sees that the basis element (P,ℓ) is present in the sum. Moreover, for any other (P',m) appearing in the sum we have $(P',m) < (P,\ell)$. Indeed, if $m>\ell$, then $p_\ell-\ell+m > p_\ell$, so the smallest ℓ elements in P' are lexicographically larger than the smallest ℓ elements in P, meaning $(P',m)<(P,\ell)$ by rule 1; if $m<\ell$, then $p_m \le p_\ell-\ell+m < p_\ell$, so the m smallest elements of P' and P are equal, meaning $(P',m)<(P,\ell)$ by rule 2. Therefore, the basis element (P,ℓ) is in the image. This argument shows that A_{i_1} has full rank. Moreover, this argument shows that, up to a permutation of the rows and columns, the matrix A_{i_1} is upper triangular with ones on the diagonal. Repeating this argument with general values for α_{i_1,i_2,i_3} proves the claim. ◀

▶ Remark. The lower bound in Theorem 20 improves a lower bound of Ikenmeyer on the border support rank of IMM_n^3 [11, 8.2.17].

5 Strassen's laser method for iterated matrix multiplication

In this section we show that $\mathrm{NQ}(\mathrm{EQ}_n^{C_k}) < kn$ for odd k. We will prove this result in the language of algebraic complexity theory.

▶ **Definition 21.** Define $\omega_k := \inf\{\alpha \in \mathbf{R} \mid \mathrm{R}(\mathrm{IMM}_n^k) \in \mathcal{O}(n^\alpha)\}$. We call this the *exponent* of iterated matrix multiplication. Define $\omega_{\mathrm{s},k} := \inf\{\alpha \in \mathbf{R} \mid \mathrm{R_s}(\mathrm{IMM}_n^k) \in \mathcal{O}(n^\alpha)\}$. We call this the *support rank exponent* of iterated matrix multiplication.

Asymptotically, we have $\mathrm{NQ}(\mathrm{EQ}_n^{C_k}) \le \omega_{\mathrm{s},k}\, n + \mathcal{O}(1) \le \omega_k\, n + \mathcal{O}(1)$. The exponents ω_3 and $\omega_{\mathrm{s},3}$ are known as ω and ω_{s} in the literature. The support rank exponent of matrix multiplication was first studied by Cohn and Umans [9]. The best upper bound on ω_s comes from the upper bound $\omega \le 2.3728639$ of Le Gall [14]. Interestingly, Cohn and Umans show the relationship

$$\omega \le (3\omega_{\mathrm{s}} - 2)/2.$$

Therefore, one way of finding upper bounds on ω is to construct an efficient quantum communication protocol for the cyclic equality problem $\mathrm{EQ}_n^{C_3}$. On the other hand, this observation indicates that improving the bounds on the quantum communication complexity of $\mathrm{EQ}_n^{C_k}$ is a hard problem.

For any k we have $k-1 \le \omega_k \le k$, and if k is even, then $\omega_k = k$ (Proposition 18). The aim of this section will be to show: if $k \ge 3$ is odd, then

$$\omega_k < k.$$

Schönhage τ-theorem. In this section we will generalize some tools for obtaining upper bounds on the exponent of ω_3 to all exponents ω_k, in particular, we generalize the Schönhage τ-theorem. The proofs in this section are straightforward generalizations of the proofs for $k = 3$ which can be found in [5]. In the next paragraph, we will use Strassen's laser method to show that $\omega_k < k$ for all odd k.

First we recall an important relationship between border rank and rank. We use the following more precise notion of border rank. Let $h \in \mathbf{N}$ and let t be a tensor in $\mathbf{C}^{\otimes m_1} \otimes \cdots \otimes \mathbf{C}^{\otimes m_k}$. Define $\mathrm{R}_h(t)$ to be the minimum number r such that there exist vectors $v_i^j \in (\mathbf{C}[\varepsilon])^{m_j}$ that satisfy $\sum_{i=1}^r v_i^1 \otimes \cdots \otimes v_i^k = \varepsilon^h t + \mathcal{O}(\varepsilon^{h+1})$. A well-known but nontrivial result is that $\underline{\mathrm{R}}(t) = \min_h \mathrm{R}_h(t)$. It is not hard to show that $\mathrm{R}_{h+h'}(t \otimes t') \leq \mathrm{R}_h(t)\,\mathrm{R}_{h'}(t')$. The relationship we are talking about is the following.

▶ **Proposition 22.** *For every $h, k \in \mathbf{N}$, there is a number c_h such that for all tensors $t \in \mathbf{C}^{m_1} \otimes \cdots \otimes \mathbf{C}^{m_k}$, $\mathrm{R}(t) \leq c_h\,\mathrm{R}_h(t)$. The number c_h depends polynomially on h.*

Proof. Let t be a tensor in $\mathbf{C}^{m_1} \otimes \cdots \otimes \mathbf{C}^{m_k}$ with $\mathrm{R}_h(t) = r$. Then there are $v_i^j \in (\mathbf{C}[\varepsilon])^{m_j}$ such that

$$\sum_{i=1}^{r} v_i^1 \otimes \cdots \otimes v_i^k = \varepsilon^h t + \mathcal{O}(\varepsilon^{h+1}).$$

Decomposing every v_i^j into ε-homogeneous components $v_i^j = \sum_{a_j=0}^{h} \varepsilon^{a_j} v_i^j(a_j)$, and collecting powers of ε gives

$$\sum_{i=1}^{r} \sum_{a_1,\ldots,a_k \in [h]} \varepsilon^{a_1+\cdots+a_k}\, v_i^1(a_1) \otimes \cdots \otimes v_i^k(a_k) = \varepsilon^h t + \mathcal{O}(\varepsilon^{h+1}).$$

Taking only the summands such that $a_1 + \cdots + a_k = h$ gives a rank decomposition of t. There are $\binom{h+k-1}{k-1} r$ such summands. ◀

Next, we show that an upper bound on the border rank of 'unbalanced' iterated matrix multiplication tensors yields and upper bound on ω_k. Define the tensor $\langle n_1, n_2, \ldots, n_k \rangle$ to be

$$\sum_{x \in [n_1] \times \cdots \times [n_k]} |x_1 x_2\rangle\, |x_2 x_3\rangle \cdots |x_k x_1\rangle\,.$$

So $\mathrm{IMM}_n^k = \langle n, n, \ldots, n \rangle$ (n occurs k times).

▶ **Proposition 23.** *If $\underline{\mathrm{R}}(\langle n_1, n_2, \ldots, n_k \rangle) \leq r$, then $\omega_k \leq k \log_{n_1 \cdots n_k} r$.*

Proof. Let $N = n_1 \cdots n_k$. There is an h such that $\mathrm{R}_h(\langle n_1, \ldots, n_k \rangle) \leq r$. By taking the tensor product of all cyclic shifts of $\langle n_1, \ldots, n_k \rangle$, we get $\mathrm{R}_{kh}(\langle N, \ldots, N \rangle) \leq r^k$ and thus $\mathrm{R}_{khs}(\langle N^s, \ldots, N^s \rangle) \leq r^{ks}$ for all s. Hence $\mathrm{R}(\langle N^s, \ldots, N^s \rangle) \leq c_{khs} r^{ks}$ for some number c_{khs} which is constant in N. Therefore,

$$\omega \leq \log_{N^s}(c_{khs} r^{ks}) = ks \log_{N^s}(r) + \log_{N^s}(c_{khs}).$$

If s goes to infinity then $\log_{N^s}(c_{khs})$ goes to zero, so $\omega_k \leq k \log_N(r)$. ◀

The real workhorse is the following straightforward generalization of a theorem of Schönhage [16].

▶ **Proposition 24** (k-party Schönhage τ-theorem). *Suppose that $r > p$ and*

$$\underline{\mathrm{R}}\Big(\bigoplus_{i=1}^{p}\langle n_1^i, n_2^i, \ldots, n_k^i\rangle\Big) \leq r.$$

Define τ by $\sum_{i=1}^{p}\big(\prod_{j=1}^{k} n_j^i\big)^{\tau} = r$. Then $\omega_k \leq k\tau$

We follow the proof of [5]. We first prove two lemmas. For tensors $s, t \in \mathbf{C}^{m_1}\otimes\cdots\otimes\mathbf{C}^{m_k}$, let $s \leq t$ denote the existence of an SLOCC transformation mapping t to s. Let $a, b \in \mathbf{N}+1$.

▶ **Lemma 25.** *Let t be a tensor such that $\mathrm{R}(t^{\oplus a}) \leq b$. Then for all s, $\mathrm{R}((t^{\otimes s})^{\oplus a}) \leq \lceil b/a\rceil^s a$.*

Proof. We prove the lemma by induction over s. The base case $s = 1$ follows from the assumption. For the induction step, we have

$$(t^{\otimes s+1})^{\oplus a} = t^{\oplus a}\otimes t^{\otimes s} \leq \mathrm{GHZ}_b \otimes t^{\otimes s} = (t^{\otimes s})^{\oplus b},$$

and thus, by the induction hypothesis,

$$\mathrm{R}((t^{\otimes s+1})^{\oplus a}) \leq \mathrm{R}((t^{\otimes s})^{\oplus b}) \leq \mathrm{R}((t^{\otimes s})^{\oplus(\lceil b/a\rceil a)}) \leq \lceil\tfrac{b}{a}\rceil\lceil\tfrac{b}{a}\rceil^s a \leq \lceil\tfrac{b}{a}\rceil^{s+1} a,$$

proving the lemma. ◀

▶ **Lemma 26.** *If $\mathrm{R}(\langle n_1, n_2, \ldots, n_k\rangle^{\oplus a}) \leq b$, then $\omega_k \leq k\log_{n_1\cdots n_k}\lceil b/a\rceil$.*

Proof. The inequality $\mathrm{R}(\langle n_1, n_2, \ldots, n_k\rangle^{\oplus a}) \leq b$ implies by Theorem 25 the inequality $\mathrm{R}(\langle n_1^s, n_2^s, \ldots, n_k^s\rangle^{\oplus a}) \leq \lceil b/a\rceil^s a$ which by Proposition 23 yields

$$\omega_k \leq k\frac{s\log\lceil\frac{b}{a}\rceil + \log(a)}{s\log(n_1\cdots n_k)},$$

which goes to $k\log\lceil b/a\rceil/\log(n_1\cdots n_k)$ when s goes to infinity. ◀

Proof of Proposition 24. We assume $\underline{\mathrm{R}}\big(\bigoplus_{i=1}^{p}\langle n_1^i, n_2^i, \ldots, n_k^i\rangle\big) \leq r$. This implies that there is an $h \in \mathbf{N}$ such that $\mathrm{R}_h\big(\bigoplus_{i=1}^{p}\langle n_1^i, n_2^i, \ldots, n_k^i\rangle\big) \leq r$. Taking the sth tensor power gives $\mathrm{R}_{hs}\big((\bigoplus_{i=1}^{p}\langle n_1^i, n_2^i, \ldots, n_k^i\rangle)^{\otimes s}\big) \leq r^s$. We expand the tensor power to get

$$\mathrm{R}_{hs}\Big(\bigoplus_{\sigma}\Big(\bigotimes_{i=1}^{p}\langle (n_1^i)^{\sigma_i}, (n_2^i)^{\sigma_i}, \ldots, (n_k^i)^{\sigma_i}\rangle\Big)^{\oplus\binom{s}{\sigma_1,\ldots,\sigma_p}}\Big) \leq r^s,$$

where the first direct sum is over all p-tuples σ of nonnegative integers with sum s. We can also write this inequality as

$$\mathrm{R}_{hs}\Big(\bigoplus_{\sigma}\langle \textstyle\prod_i (n_1^i)^{\sigma_i}, \ldots, \prod_i (n_k^i)^{\sigma_i}\rangle^{\oplus\binom{s}{\sigma_1,\ldots,\sigma_p}}\Big) \leq r^s.$$

There exists a number c_{hs} depending polynomially on h and s such that

$$\mathrm{R}\Big(\bigoplus_{\sigma}\langle \textstyle\prod_i (n_1^i)^{\sigma_i}, \ldots, \prod_i (n_k^i)^{\sigma_i}\rangle^{\oplus\binom{s}{\sigma_1,\ldots,\sigma_p}}\Big) \leq c_{hs}\, r^s.$$

Define τ by $\sum_{i=1}^{p}\big(\prod_{j=1}^{k} n_j^i\big)^{\tau} = r$. Then $\sum_{\sigma}\binom{s}{\sigma_1,\ldots,\sigma_p}\big(\prod_i (n_1^i)^{\sigma_i}\cdots\prod_i (n_k^i)^{\sigma_i}\big)^{\tau} = r^s$. In this sum, consider the maximum summand and fix the corresponding σ. Define the numbers $n_j \coloneqq \prod_i (n_j^i)^{\sigma_i}$. Let $a \coloneqq \binom{s}{\sigma_1,\ldots,\sigma_p}$ and $b \coloneqq r^s c_{hs}$. We apply Theorem 26 to the inequality $\mathrm{R}(\langle n_1, \ldots, n_k\rangle^{\oplus a}) \leq b$ to obtain

$$\omega_k \leq k\tau + \frac{(p-1)\log(s+1) + \log(c_{hs})}{\log(n_1\cdots n_k)},$$

which goes to $k\tau$ when s goes to infinity. (See [5] for more details.) ◀

Strassen's laser method. We will now use Strassen's laser method to prove the main result of this section.

▶ **Theorem 27.** *For any odd k we have $\omega_k < k$.*

We will give a proof for the case $k = 5$, the other cases being similar. Define the 5-tensor $\mathrm{Str}_q^5 = \sum_{i=1}^q |ii000\rangle + |0ii00\rangle$ in $\mathbf{C}^{q+1} \otimes \mathbf{C}^q \otimes \mathbf{C}^{q+1} \otimes \mathbf{C} \otimes \mathbf{C}$.

▶ **Proposition 28.** $\underline{\mathrm{R}}(\mathrm{Str}_q^5) \leq q + 1$.

Proof. Expanding $\sum_{i=1}^q (|0\rangle + \varepsilon\,|i\rangle)\,|i\rangle\,(|0\rangle + \varepsilon\,|i\rangle)\,|0\rangle|0\rangle$ gives

$$\sum_{i=1}^{q} |0i000\rangle + \varepsilon \sum_{i=1}^{q} |ii000\rangle + |0ii00\rangle + \mathcal{O}(\varepsilon^2).$$

Subtracting $|0\rangle\big(\sum_{i=1}^q |i\rangle\big)|000\rangle$ yields $\varepsilon\,\mathrm{Str}_q^5 + \mathcal{O}(\varepsilon^2)$. ◀

▶ **Proposition 29.** $\mathrm{GHZ}_2^5 \leq \langle 2,2,2,2,2\rangle$.

Proof. Let ϕ be the map $|ab\rangle \mapsto \delta_{[a=b]}\,|a\rangle$. Apply $\phi^{\otimes 5}$ to $\langle 2,2,2,2,2\rangle$. This yields one copy of $\mathrm{GHZ}_2^{[5]}$. ◀

▶ Remark. We mention that the subrank result of Proposition 29 can by improved asymptotically in the sense that $\omega(\langle 2,2,2,2,2\rangle, \mathrm{GHZ}^5) = 1/2$ [20]. Using this fact in the proof of Theorem 27 gives the slightly better upper bound $\omega_k \leq \log_q((q+1)^k/4)$.

For the proof of Theorem 27 we have to define the notion of the decomposition of the support of a tensor and the corresponding inner and outer structure of a tensor. Let $I_1, \ldots, I_k$ be finite sets. A *decomposition* $\mathcal{D}$ of $I_1 \times \cdots \times I_k$ is a collection of sets I_i^j such that

$$I_i = \bigsqcup_j I_i^j,$$

meaning that for every i, $\cap_j I_i^j = \emptyset$ and $\cup_j I_i^j = I_i$. Let t be a tensor in $\mathbf{C}^{m_1} \otimes \cdots \otimes \mathbf{C}^{m_k}$ and index the basis elements in this space by elements of $[m_1] \times \cdots \times [m_k]$. Let $\mathcal{D}$ be a decomposition of $[m_1] \times \cdots \times [m_k]$. We view $\mathcal{D}$ as a 'cut' of $[m_1] \times \cdots \times [m_k]$ into smaller product sets and thus as a 'cut' of t into smaller tensors. We define $t|_{I_1^{j_1}, I_2^{j_2}, \ldots, I_k^{j_k}}$ to be the restriction of t to the basis elements in $I_1^{j_1} \times I_2^{j_2} \times \ldots \times I_k^{j_k}$. These smaller tensors we think of as the 'inner structure' of t. We define the 'outer structure' of t with respect to $\mathcal{D}$ to be the tensor $t_{\mathcal{D}}$ indexed by sequences $(j_1, \ldots, j_k)$ such that $t_{\mathcal{D}}$ has a 1 at position $(j_1, \ldots, j_k)$ if t restricted to $I_1^{j_1} \times \cdots \times I_k^{j_k}$ is not the zero tensor, and a 0 otherwise.

Proof of Theorem 27. We will give a proof for the case $k = 5$, the other cases being similar. Define a block decomposition $\mathcal{D}$ of the support $I_1 \times \cdots \times I_5$ of Str_q^5 by

$$I_1 = \{0\} \cup \{1, \ldots, q\}$$
$$I_2 = \{1, \ldots, q\}$$
$$I_3 = \{0\} \cup \{1, \ldots, q\}$$
$$I_4 = \{0\}$$
$$I_5 = \{0\}.$$

We have the outer structure $(\mathrm{Str}_q^5)_{\mathcal{D}} = |11000\rangle + |01100\rangle \cong |10100\rangle + |00000\rangle$. Note that this is just an EPR pair between party 1 and 3. The inner structures are $\sum_{i=1}^q |ii000\rangle$ and

$\sum_{i=1}^{q} |0ii00\rangle$, which are also known as $\langle 1, q, 1, 1, 1\rangle$ and $\langle 1, 1, q, 1, 1\rangle$. Let Cyc_5 be the map $t \mapsto t \otimes \sigma t \otimes \sigma^2 t \otimes \sigma^3 t \otimes \sigma^4 t$ with $\sigma = (12345)$. Let $\hat{\mathcal{D}} = \mathrm{Cyc}_5 \mathcal{D}$ be the naturally corresponding decomposition. Then

$$\langle 2, 2, 2, 2, 2\rangle^{\otimes s} = (\mathrm{Cyc}_5 \operatorname{Str}_q^5)^{\otimes s}_{\hat{\mathcal{D}}^{\otimes s}} \quad \text{and} \quad \underline{\mathrm{R}}\big((\mathrm{Cyc}_5 \operatorname{Str}_q^5)^{\otimes s}\big) \leq (q+1)^{5s}. \tag{1}$$

Note how the first statement relies on 5 being odd.

The inner structure of $(\mathrm{Cyc}_5 \operatorname{Str}_q^5)^{\otimes s}_{\hat{\mathcal{D}}^{\otimes s}}$ consists of tensors from $I \coloneqq \{\langle n_1, n_2, n_3, n_4, n_5\rangle \mid n_1 \cdots n_5 = q^{5s}\}$. Combining equation (1) with Proposition 29 gives that there are 2^s elements $t_1, t_2, \ldots \in I$ such that

$$\underline{\mathrm{R}}(t_1 \oplus t_2 \oplus \cdots) \leq (q+1)^{5s}.$$

Now the τ-theorem says that if we define τ by

$$2^s (q^{5s})^{\tau} = (q+1)^{5s}$$

then $\omega_5 \leq 5\tau$. Therefore,

$$\omega_5 \leq 5\tau \leq \log_q \frac{(q+1)^5}{2}$$

which gives $\omega_5 \leq 4.84438$. In general, one gets $\omega_k \leq \log_q \frac{(q+1)^k}{2}$ which is strictly smaller than k for q large enough. ◀

Acknowledgements. We thank Peter Bürgisser, Péter Vrana, Florian Speelman and Teresa Piovesan for helpful discussions.

References

1. Andris Ambainis, Harry Buhrman, Yevgeniy Dodis, and Hein Röhrig. Multiparty quantum coin flipping. In *Computational Complexity, 2004. Proceedings. 19th IEEE Annual Conference on*, pages 250–259. IEEE, 2004. arXiv:quant-ph/0304112, doi:10.1109/CCC.2004.1313848.
2. Michael Ben-Or and Richard Cleve. Computing algebraic formulas using a constant number of registers. *SIAM Journal on Computing*, 21(1):54–58, 1992. doi:10.1137/0221006.
3. Amey Bhangale and Swastik Kopparty. The complexity of computing the minimum rank of a sign pattern matrix. *arXiv preprint arXiv:1503.04486*, 2015. arXiv:1503.04486.
4. Markus Bläser. Complete problems for Valiant's class of qp-computable families of polynomials. In *Computing and Combinatorics*, pages 1–10. Springer, 2001. doi:10.1007/3-540-44679-6_1.
5. Markus Bläser. Fast matrix multiplication. *Theory of Computing, Graduate Surveys*, 5:1–60, 2013. doi:10.4086/toc.gs.2013.005.
6. Peter Bürgisser, Michael Clausen, and M. Amin Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1997. With the collaboration of Thomas Lickteig. doi:10.1007/978-3-662-03338-8.
7. Eric Chitambar, Runyao Duan, and Yaoyun Shi. Tripartite entanglement transformations and tensor rank. *Physical review letters*, 101(14):140502, 2008. arXiv:0805.2977, doi:10.1103/PhysRevLett.101.140502.
8. Matthias Christandl and Jeroen Zuiddam. Tensor surgery and tensor rank. *arXiv preprint arXiv:1606.04085*, 2016. arXiv:1606.04085.

9 Henry Cohn and Christopher Umans. Fast matrix multiplication using coherent configurations. In *Proceedings of the Twenty-fourth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA'13, pages 1074–1086, Philadelphia, PA, USA, 2013. Society for Industrial and Applied Mathematics. URL: http://dl.acm.org/citation.cfm?id=2627817.2627894, arXiv:1207.6528.

10 Fulvio Gesmundo. Geometric aspects of iterated matrix multiplication. *Journal of Algebra*, 461:42–64, 2016. arXiv:1512.00766, doi:10.1016/j.jalgebra.2016.04.028.

11 Christian Ikenmeyer. *Geometric complexity theory, tensor rank, and Littlewood-Richardson coefficients*. PhD thesis, Universität Paderborn, 2013. URL: http://nbn-resolving.de/urn:nbn:de:hbz:466:2-10472.

12 Joseph M. Landsberg and Mateusz Michałek. On the geometry of border rank algorithms for matrix multiplication and other tensors with symmetry. *arXiv preprint arXiv:1601.08229*, 2016. arXiv:1601.08229.

13 Joseph M. Landsberg and Giorgio Ottaviani. New lower bounds for the border rank of matrix multiplication. *Theory Comput.*, 11:285–298, 2015. arXiv:1112.6007, doi:10.4086/toc.2015.v011a011.

14 François Le Gall. Powers of tensors and fast matrix multiplication. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC'14, pages 296–303, New York, NY, USA, 2014. ACM. doi:10.1145/2608628.2608664.

15 Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

16 Arnold Schönhage. Partial and total matrix multiplication. *SIAM Journal on Computing*, 10(3):434–455, 1981. doi:10.1137/0210032.

17 Volker Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356, 1969. doi:10.1007/BF02165411.

18 Volker Strassen. Rank and optimal computation of generic tensors. *Linear algebra and its applications*, 52:645–685, 1983. doi:10.1016/0024-3795(83)80041-X.

19 Marcos Villagra, Masaki Nakanishi, Shigeru Yamashita, and Yasuhiko Nakashima. Tensor rank and strong quantum nondeterminism in multiparty communication. In *Theory and applications of models of computation*, volume 7287 of *Lecture Notes in Comput. Sci.*, pages 400–411. Springer, Heidelberg, 2012. arXiv:1202.6444, doi:10.1007/978-3-642-29952-0_39.

20 Péter Vrana and Matthias Christandl. Entanglement distillation from Greenberger-Horne-Zeilinger shares. *arXiv preprint arXiv:1603.03964*, 2016. arXiv:1603.03964.

21 Ronald de Wolf. Nondeterministic quantum query and communication complexities. *SIAM Journal on Computing*, 32(3):681–699, 2003. arXiv:cs/0001014, doi:10.1137/S0097539702407345.